

# OUCH!

## BU SAYIDA...

- Kendinizin Güvenliğini Sağlamak
- Bilgisayarlarınızın ve Hesaplarınızın Güvenliğini Sağlamak
- Aileler İçin

## Çevrimiçi Oyunları Güvenle Oynamak

### Genel Bakış

Çevrimiçi oyunlar eğlenmek için harika bir seçimdir ancak kendine özel risklerle birlikte gelir. Bu bültende, çevrimiçi oyunlar oynarken kendinizi ve ailenizi korumak için yapabileceğinizden bahsedeceğiz.

### Kendinizin Güvenliğini Sağlamak

Çevrimiçi oyunları o kadar ilgi çekici kılan, dünyanın her yerinden gelen yabancılar ile iletişim kurmak ve oyun oynamak olabilir. Çoğu zaman birlikte oynadığınız insanların kimler olduğunu bilmezsiniz. Çevrimiçi kişilerin büyük çoğunluğu sizin gibi eğlenmek için orada olabilirler ancak aralarında zarar vermek isteyenler de vardır. Güvenli kalmak için yapmanız gereken bazı şeyler:

- Bir bağlantıyı tıklamanız ya da bir dosyayı indirmeniz gibi herhangi bir aksiyon almanızı isteyen her mesaja şüphe ile yaklaşın. Ortalama saldırıları gibi kötü niyetli kişiler bilgisayarınızı ele geçirmek için sizi kandırmayı denemeye devam edeceklerdir. Eğer bir mesaj, çok acil, gerçek olamayacak kadar güzel ya da tuhaf ise, mutlaka bir saldırı olabileceği yönünde şüphelenin.
- Pek çok çevrimiçi oyunun, ticari takas ya da sanal mal satın alabileceğiniz kendi mali piyasaları vardır. Bu sistemlerde tıpkı gerçek dünyadaki gibi, sizi paranız için kandırmaya çalışan ya da düpedüz onu çalmak için uğraşan dolandırıcılar bulunur.
- Oyun içi satın alma yapılan işlemlerde dikkatli olun. Bu hareketleri sadece itibarlı platformlarda yapın.
- Çevrimiçiyken, kendiniz ve çocuklarınız hakkında paylaştığınız bilgileri sınırlayın. Şifreleriniz ya da ev adresleriniz gibi kişisel bilgilerinizi asla paylaşmayın.
- Birçok web sitesi, örneğin bankacılık siteleri, kimliğinizi doğrulamaya yardımcı olmak için güvenlik soruları kullanır. Saldırganların çevrimiçi arkadaşlıkları kurbanlarının güvenlik sorularının cevaplarını almak için kullandıkları bilinmektedir. İnsanların sizinle oyun oynarken sordukları soruları cevaplama zorunluluğunuzun olmadığını unutmayın.

### Bilgisayarlarınızın ve Hesaplarınızın Güvenliğini Sağlamak

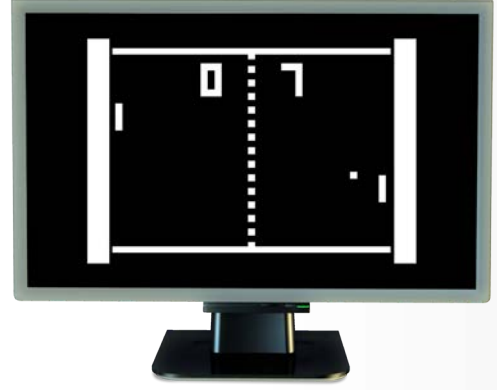
Bir sonraki adım kullandığınız bilgisayarı güvenli hale getirmektir. Kötü niyetli kişiler bilgisayarınızı ya da oyunlarda kullandığınız hesaplarınızı ele geçirmeyi deneyeceklerdir, onları korumalısınız.

### Konuk Yazar

Jake Williams Rendition Infosec'in kurucusu ve baş danışmanı, sertifikalı SANS eğitmeni ve birçok SANS eğitiminin ortak yazarıdır. Twitter'da [@MalwareJake](#) hesabıyla aktiftir ve düzenli olarak [malwarejake.blogspot.com](http://malwarejake.blogspot.com) adresinde yazılarını paylaşmaktadır.

## Çevrimiçi Oyunları Güvenle Oynamak

- Bilgisayarınız ve tüm oyun hesaplarınız için güçlü parola kullanın. Böylece saldırganlar parolalarınızı kolayca tahmin edip, hesaplarınızı ele geçiremezler. Eğer oyun size iki aşamalı doğrulama seçeneği sunuyorsa, kullanın. Ek olarak, her oyun hesabınızın parolasının farklı olduğundan emin olun. Böylelikle, eğer parolanız bir oyun için açığa çıkarsa, diğer hesaplarınız güvende kalır.
- Daima işletim sisteminin ve oyun yazılımının son sürümünü çalıştırarak bilgisayarınızın güvenliğini sağlayın. Tıpkı işletim sistemi ve web tarayıcınız gibi, eski ve önceki sürümlere ait oyun yazılımlarının saldırganların istismar edebileceği bilinen açıkları vardır. Bilgisayarınızı ve oyun yazılımlarınızı güncel tutarak, bilinen güvenlik açıklarının birçoğunu ortadan kaldırmış olursunuz.
- Anti virüs yazılımı kullanın ve güncelliği ile gerçek zamanlı dosya kontrollü koruma sağladığından emin olun.
- Sadece güvenilir sitelerden oyun yazılımları indirin. Eğer oyun oynamak için bir yazılım kuruyorsanız, sağlayıcısının sitesinden ya da iyi bilinen, güvenilir bir siteden indirdiğinizden emin olun. Sıklıkla, siber saldırganlar oyun sitelerinin, sahte ya da kötü niyetli kod eklenmiş bir versiyonunu hazırlar ve kendi sunucularından dağıtırlar. Eğer bunlardan birini kurarsanız, bilgisayarınızın kontrolünü ele geçirirler.
- Oyunlara yeni özellikler eklemek için alınan ek paketler, genellikle topluluklar tarafından geliştirilir. Saldırganlar, bazen anti- virus yazılımlarının bulmasının çok zor olduğu kötü niyetli kodlar bulaştırılmış oyun ek paketleri hazırlar. Tıpkı oyunları indirirken yapmanız gerektiği gibi ek paketleri de sadece güvenli yerlerden indirin. Ek olarak, herhangi bir ek paket anti-virus yazılımınızı pasif hale getirmenizi ya da firewall ayarlarınızı değiştirmenizi isterse, onu kullanmayın.
- Yeraltı piyasalar, hileli aktiviteleri desteklemek için çoğaldılar. Etik dışı olmanın yanısıra buralarda kullanılan birçok programın kendisi, en tehlikeli kötü niyetli yazılım araçları (rootkit) halinde. Hiçbirini kurmayın ve kullanmayın.
- Hangi çevrimiçi oyun yazılımını kullanıyorsanız, web sitelerini kontrol edin. Birçok oyun sitesinin, kendinizi ve sistemlerinizi nasıl güvenli hale getireceğiniz ile ilgili sayfaları bulunur, oradaki tavsiyelere uyduğunuzdan emin olun.
- Son olarak, mobil cihazlarınızda da oyun oynarken tıpkı bilgisayarınızda oynuyor gibi dikkatli olun. Siber saldırganlar artık, mobil cihazlarınızı hedef almaya başladı.



*Çevrimiçi oyunlar oynarken güvenli kalmanın anahtarı güçlü parolalar kullanmak, bilgisayarınızın güvenliğini sağlamak ve yabancılarla konuşurken ya da size özel bir mesaj / davet aldığınızda sağduyunuzu kullanmaktır.*

## Çevrimiçi Oyunları Güvenle Oynamak

### Aileler İçin

Eğer bir ebeveyn iseniz, çocuklarınızın yukarıda bahsettiğimiz adımları izlediğinden emin olun. Ek olarak, çocuklarınızla riskler hakkında konuşun. Eğitim ve açık iletişim, çocuklarınızı korumak için atabileceğiniz en etkili adımdır. Çocuklarınızı konuşturabilmenin en sık kullanılan yöntemi, onlara oyunlarının nasıl oynandığını sormanız, kendileri ile birlikte onların çevrimiçi dünyalarında yürümeniz ve size o oyunların neye benzediğini göstermelerini sağlamanızdır. Hatta oyunları onlarla birlikte oynayabilirsiniz. Ayrıca, çevrimiçiyken tanıştıkları değişik insanlardan bahsetmelerini isteyin. Sıklıkla çevrimiçi oyunlar çocuğunuzun sosyal hayatının büyük bir parçasını oluşturuyor olabilir. Onlarla konuşarak ve onların sizinle konuşmalarını sağlayarak problemleri ortaya çıkarabilir ve onları, herhangi bir teknolojiden çok daha etkin bir şekilde koruyabilirsiniz.

### Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve

<http://www.securingthehuman.org> adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

### Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

### Kaynaklar

Şifreler:	<a href="http://www.securingthehuman.org/ouch/2014#november2014">http://www.securingthehuman.org/ouch/2014#november2014</a>
İki Adımlı Doğrulama:	<a href="http://www.securingthehuman.org/ouch/2013#february2013">http://www.securingthehuman.org/ouch/2013#february2013</a>
Şifreleme:	<a href="http://www.securingthehuman.org/ouch/2013#october2013">http://www.securingthehuman.org/ouch/2013#october2013</a>
Tabletinizi Güvenli Hale Getirmek:	<a href="http://www.securingthehuman.org/ouch/2014#december2014">http://www.securingthehuman.org/ouch/2014#december2014</a>
Verizon DBIR 2014:	<a href="http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips">http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips</a>

OUCH!, SANS Securing The Human Programı tarafından yayınlanır ve [Creative Commons BY-NC-ND 4.0 lisansı](https://creativecommons.org/licenses/by-nc-nd/4.0/) altında dağıtılır. Bülteni değiştirmediniz sürece, bu bülteni dağıtabilir ya da kendi farkındalık programlarınızda kullanabilirsiniz. Çeviri ya da daha fazla bilgi için, lütfen [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org) e-posta adresini kullanarak iletişime geçiniz.

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org/)